# .BR DNSSEC Update

ICANN 53 – Buenos Aires – DNSSEC Workshop

2015-06-24

Rubens Kuhl <rubens@registro.br>
Product Manager

# .br DNSSEC short story

2007-05-04 .br initially signed
    With other 4 small second level zones

2009-01-15 .[com|org].br signed
    In the advent of nsec3/opt-out
    All zones signed

2010-05-31 first KSK roll
    New Ceremony with using HSMs

2010-06-23 .br DS hit the root

2010-11-25 Started to provide DNSSEC hosting for limited size zones

# KSK Rollover

DPS mandates KSK use from 2 to 5 years. This is our first rollover after root was signed. No algorithm rollover still using RSA/SHA1.

Updated DPS increased keys size [KZC]SK

.br KSK is now 1536 bits
.br ZSK is now 1280 bits
*.br CSK is now 1280 bits

Rollover started at 2014-12-08 ceremony 2015-1. Key was added to the zone at 2015-05-18, DS with a new hash algorithm was added to the root at 2015-05-20, old DS was removed from the root at 2015-06-18. The old key will be removed from the zone at 2015-07-13.

# DNSSEC Scalability

From time to time a message finds one of the DNS mailing lists telling how DNSSEC is not deployed because it could not scale.

This is far from the truth. Since the beginning, deployment tools have evolved. A lot.

This is one data point: adequate architecture and a single modest machine by today terms, 4 Cores 4 GB RAM, handles backend zone editing , key generation, signing/resigning and DNS hidden master for a fleet of 12 auth servers for 700k zones.

http://registro.br/dnsshim/index-EN.html

# DANE SMTP

Promoted with a presentation at the last GTER, the Brazilian Network Operators Meeting, with the launch of an updated “wizard” that auto generate TLSA records at our zone management interface.

The new version works for HTTPS and SMTP.

It continues to look for certificates at port 443 of A/AAAA and if there is MX records or A/AAAA records at the apex, connects at port 25 gives an EHLO looking for STARTTLS capability and if present upgrades the connection looking for certificates and then generate the TLSA records at the zone.

Questions?

Thanks!